REMARKS

Applicant appreciates the Office Action of August 9, 2005. Applicant respectfully requests reconsideration and withdrawal of the rejections with respect to the pending claims for at least the reasons discussed herein.

Independent Claims 1, 13 and 14 are Patentable over the Cited Combination

Claims 1-5 and 11-14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Application Publication No. 2002/0034301 to Andersson (hereinafter "Andersson"), in view of United States Application Publication No. 2004/0202328 to Hara (hereinafter "Hara"). *See* Office Action, page 2. Applicant respectfully submits that many of the recitations of these claims are neither disclosed nor suggested by the cited combination. For example, Claim 1 recites:

> A method for authentication of a user by an authenticating entity comprising the steps of:
> the authenticating entity sending a challenge to the user;
> **the user adding a spoiler to the challenge;**
> **the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;**
> **the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.**

Claims 13 and 14 contain corresponding system and computer program product recitations, respectively. Applicant respectfully submits that at least the highlighted recitations of Claim 1 are neither disclosed nor suggested by the cited combination for at least the reasons discussed herein.

The Office Action states that Andersson teaches all the recitations of Claim 1 except for "adding a spoiler to the challenge and encrypting the combined spoiler and challenge." *See* Office Action, page 2. However, the Office Action points to Hara as providing the missing teachings. *See* Office Action, page 3. Applicant respectfully disagrees. In particular, the cited portion of Andersson discusses a conventional encryption system that includes sending a challenge to the requesting party. *See* Andersson, page 3, paragraph 40. In fact, this type of conventional encryption system is discussed in the Background of the present application. *See* Figure 2 and corresponding text. Applicant does not dispute that the use of a challenge as

discussed in Andersson is known. However, Claim 1 recites "**adding a spoiler** to the challenge; encrypting the **combined spoiler and challenge** using a private key of an asymmetric key pair and sending a response to the authenticating entity **in the form of the encrypted combined spoiler and challenge**. Nothing in Andersson discloses or suggests at least these recitations of Claim 1. Furthermore, Hara does not provide the missing teachings.

In particular, the cited portion of Hara states:

> [0083] As shown in FIG. 7B, the data transmitter 2 performs data encapsulation in accordance with the first protocol **first by padding the IP datagram (i.e., adding a padding part 102) to make the length of the data part an integer multiple of 64 bits**. For example, a padding part of 0 to 63 bits is suffixed to the IP datagram 101. **All bits in the padding part are "1" each.** The padding is intended to **keep the datagram to a predetermined data length because the data part is better suited for encryption when its length is an integer multiple of 64 bits**. The data part placed in the format of the first protocol is called a section hereunder.
>
> [0084] The section supplemented with the padding 102 is then encrypted by the data transmitter 2 as shown in FIG. 7C. Encryption is carried out by use of encryption keys. The encryption keys are session keys (described later) used to encrypt information to be sent to the data receiver 3. The encryption method adopted here is a block encryption method based on the common key cryptosystem such as the Triple-DES. The Triple-DES encryption is one of today's strongest public key cryptosystems and is easy to implement for high-speed encryption on a hardware basis. This encryption process, unlike that of most public key cryptosystems, is fast enough to keep up with transmission at rates of as high as 30 Mbps.

See Hara, paragraphs 83 and 84 (emphasis added). The cited portion of Hara discusses filling in bits in an IP datagram with "1's" so as to create a 64 bit datagram, which is better suited for encryption. Thus, Hara basically discusses adding place holders in the IP datagram. Nothing in Hara discusses the addition of a "spoiler" as recited in Claim 1. In fact, the addition of 1's discussed in Hara would not provide any added level of security as a "spoiler" that is always all 1's is easy to figure out. Accordingly, Hara does not provide the missing teachings. Accordingly, Claim 1 is patentable over the cited combination for at least these reasons.

Accordingly, none of the cited references either alone or in combination disclose or suggest many of the recitations of Claim 1 set out above. Furthermore, there is no motivation or suggestion to combine the cited references as suggested in the Office Action. As affirmed by the

Court of Appeals for the Federal Circuit in *In re Sang-su Lee*, a factual question of motivation is material to patentability, **and cannot be resolved on subjective belief and unknown authority**. *See In re Sang-su Lee*, 277 F.3d 1338 (Fed. Cir. 2002). It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to "[use] that which the inventor taught against its teacher." *W.L. Gore v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 U.S.P.Q. 303, 312-13 (Fed. Cir. 1983).

The Office Action states:

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to add padding data to the password and encrypting the password with the padding data, since Hara discloses at page 5, paragraphs [083], [0084] that padding data makes it better suited for encryption, as it is known that padding data to a certain length **makes the encryption stronger**, which is desirable when trying to prevent transmitted password information from being intercepted.

See Office Action, page 3 (emphasis added). This motivation is a motivation based on "subjective belief and unknown authority", the type of motivation that was rejected by the Federal Circuit in *In re Sang-su Lee*. In other words, the Office Action does not point to any specific portion of the cited references that would induce one of skill in the art to combine the cited references as suggested in the Office Action. In fact, the Office Action misinterprets the cited portion of Hara. Nothing in the cited portion of Hara states that the padding makes the encryption "stronger", only that a length of 64 bits is "better suited" for encryption, *i.e.*, easier to encrypt as it is a more standard length. Again, as discussed above, adding all 1's is not going to strengthen the encryption, as it would be easy to predict. Accordingly, the statement in the Office Action with respect to motivation does not adequately address the issue of motivation to combine as discussed in *In re Sang-su Lee*. Thus, it appears that the Office Action gains its alleged impetus or suggestion to combine the cited references by hindsight reasoning informed by Applicant's disclosure, which, as noted above, is an inappropriate basis for combining references.

Furthermore, Andersson discusses network authentication that uses a conventional challenge responsive to a request. *See* Andersson, page 3, paragraph 40. Hara, on the other hand, discusses a data transmission method including encryption where the header is padded

with 1's to create a 64 bit block that may be well suited for encryption. *See* Hara, paragraphs 83 and 84. Furthermore, there is no discussion of a "challenge" in the cited portion of Hara. Nothing in the cited references or the art itself would motivate a person of skill in the art to combine the network authentication application of Andersson with the data transmission application of Hara. Furthermore, even if Andersson and Hara could be properly combined, the combination of Andersson and Hara would not teach the recitations of the pending claims for at least the reasons discussed above.

Accordingly, Applicant respectfully submits that Independent Claims 1, 13 and 14 are patentable over the cited combination for at least these additional reasons. Furthermore, the dependent claims are patentable at least per the patentability of independent Claims 1, 13 and 14 from which they depend. Accordingly, Applicant submits that independent Claims 1, 13 and 14 and the claims that depend therefrom are in condition for allowance, which is respectfully requested in due course.

Many of the Dependent Claims are Separately Patentable

Dependent Claims 2-5 and 11-12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Andersson, in view of Hara. *See* Office Action, page 2. Dependent Claims 6-8 and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Andersson in view of Hara in further view of United States Patent No. 6,072,875 to Tsudik (hereinafter "Tsudik"). *See* Office Action, page 4. As discussed above, the dependent claims are patentable at least per the patentability of the independent base claims from which they depend. Furthermore, many of the dependent claims are separately patentable over the cited combination.

For example, Claim 2 recites:

> A method as claimed in claim 1, wherein the method includes the authenticating entity decrypting the encrypted **combined spoiler and challenge** using the public key of the asymmetric key pair and determining if the user has been authenticated.

As discussed above, nothing in Andersson or Hara discloses or suggests a combined spoiler and challenge as recited in the claims of the present application. Accordingly, it follows that nothing in the cited references discloses or suggests encryption of the combined spoiler and challenge as

recited in Claim 2. Accordingly, Claim 2 is separately patentable over the cited references for at least these additional reasons.

Claims 3 through 5 recite details of the spoiler. As discussed above, nothing in the cited references discloses or suggests a spoiler as recited in the claims of the present application. Accordingly, it follows that nothing in the cited references discloses or suggests details with respect to the spoiler as recited in Claims 3 through 5. Accordingly, Claims 3-5 are separately patentable over the cited references for at least these additional reasons.

Furthermore, the Office Action admits that the combination of Andersson and Hara do not disclose or suggest the recitations of Claims 6-8 and 10. *See* Office Action, pages 4-5. However, the Office Action points to Tsudik as providing the missing teachings. *See* Office Action, pages 4-5. Applicant respectfully disagrees. Claims 6-8 and 10 contain details of obtaining a digest according to some embodiments of the present invention. In particular, Claim 6 recites "obtaining a digest of the combined spoiler and challenge before the step of encrypting." The cited portions of Tsudik states:

> Communication between mobile users of and in a computer network is subject to a variety of security issues; user identification and user tracking are two particularly important ones. This invention provides a method and an apparatus for securely identifying a mobile user while avoiding trackability of his/her movements, i.e. it provides a way for a secure user identification in secrecy. The gist is to encrypt the user's identifier, and/or his/her password, and a synchronization indication, preferably a fixed time interval, under a secret one-way function and sending the encrypted message, herein called "dynamic user identifier", to the user's "home authority" where he/she is registered. The home authority comprises correspondence tables listing, pre-computed for every time interval (or another chosen synchronization), the dynamic user identifiers and the corresponding true identity of the user and can thus quickly decide whether the received encrypted message originates from a registered user. On the other hand, an intruder is neither able to detect from the encrypted messages the identity of the user nor can he/she track a user's moves.

See Tsudik, column 3, line 59 to column 4, line 11. Nothing in the cited portion of Tsudik discloses or suggests the digest recitations of Claims 6-8 and 10.

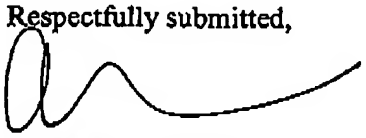
In addition, one of skill in the art would not be motivated to combine the method and apparatus for secure identification of a mobile user of Tsudik with the teachings of Andersson and Hara. The Office Action combines three references to allegedly teach the recitations of

Claims 6-8 and 10. The more references that need to be combined to allegedly teach the recitations of particular claims, the less obvious the combination becomes. It is clear that Applicant's disclosure was used as a road map to combine the cited references, which, as discussed above, is improper. Accordingly, Claims 6-8 and 10 are separately patentable over the cited combination for at least these additional reasons.

CONCLUSION

Applicant respectfully submits that pending claims are in condition for allowance for at least the reasons discussed above. Thus, allowance of the pending claims is respectfully requested in due course. Favorable examination and allowance of the present application is respectfully requested.

Respectfully submitted,



Elizabeth A. Stanek
Registration No. 48,568

USPTO Customer No. 46590
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401